METHOD AND APPARATUS FOR SIMPLIFIED AUDIO AUTHENTICATION

BACKGROUND

Priority And Related Cases

[0001] This application is related to Serial No. 09/611,569, entitled "Method and Apparatus for Secure Identity Authentication with Audible Tones", filed July 7, 2000, and claims priority to provisional patent application Serial No. 60/344,959, entitled "Method and Apparatus for Simplified Audio Authentication", filed December 21, 2001. Both applications are incorporated by reference herein.

I. Field of the Invention

[0002] The present invention pertains generally to the field of electronic security, and more particularly, to authentication of individuals through audio tones.

II. Background

[0003] Access to the Internet and use of electronic data systems have grown steadily among the general public. Electronic commerce has been eagerly embraced by both consumers and businesses due to a number of factors, such as the relative ease with which a party can buy or sell to another party without the inherent complications involved in traditional establishments.

[0004] However, along with the increase in electronic commerce, the opportunities for fraudulent activity have also increased. Misappropriated identity in the hands of wrongdoers may cause damage to innocent individuals. In worst case scenarios, a wrongdoer may actually purloin a party's identity in order to exploit the creditworthiness and financial accounts of an individual.

[0005] In order to prevent unauthorized persons from intercepting private information, various security and encryption schemes have been developed so that private information transmitted between parties is concealed. However, the concealment of private information is only one aspect of the security needed to achieve a high level of consumer confidence in electronic commerce transactions. Another aspect is authentication.

[0006] Traditionally, signatures are placed on legal documents to identify the parties involved in the subject matter of the documents and to establish that the parties are in formal agreement. With the advent of electronic commerce transactions, electronic signatures are necessary to formalize the identification of parties and the corresponding agreements between them. The

"Electronic Signatures in Global and National Commerce Act" was enacted to give such electronic signatures the same force of law as a penned signature for legal contracts. However, implementation of such secure electronic signatures has been left unresolved by the government.

[0007] Accordingly, electronic authentication of an individual may currently be performed by authentication through knowledge, such as a password or a personal identification number (PIN); authentication through portable objects, such as a credit card, or a proximity card; and/or authentication through personal characteristics (biometrics), such as a fingerprint, DNA, or a signature.

[0008] With current reliance on electronic security measures, it is not uncommon for an individual to carry multiple authentication objects or be forced to remember multiple passwords. For example, an individual may perhaps need a PIN for an ATM machine, a password to log onto a computer, a second password to access an internet service provider at home, multiple passwords to access various internet pages, a proximity card to gain access to secured buildings or structures, or a garage door opener to gain entry into a house.

[0009] Authentication through knowledge is thus problematic for individuals who are forced to remember multiple passwords or PINs. Also, passwords that are the easiest for a person to recall are the passwords that are the easiest for another person to guess. Further, security may be compromised as people may write down such information because the amount of information needed to be retained is voluminous. Writing down such information leaves an individual vulnerable to the theft of passwords or PIN codes.

[0010] Authentication through portable objects and personal characteristics may also be problematic for an average customer due to the highly specialized input devices that are required to retrieve authentication information. For example, ATM cards require an ATM machine and smart cards require a smart card reader.

[0011] Accordingly, current methods utilizing physical objects and personal characteristics are inadequate for a person who must be authenticated through a data connection or across a telephone line. In addition, having to remember passwords or carry multiple physical objects is cumbersome to the individual. Therefore, there is a present need to simplify and increase the security of the process of authenticating an individual.

SUMMARY

[0012] An apparatus that may be used by an individual to securely identify oneself by emitting a secure identifier is disclosed. The identification and authentication process is one-way; that is, the individual transmits a secure identifier, the receiver then authenticates the secure identifier, and permits access. The secure identifier comprises a digital signature, a time element, and a key identifier. The apparatus comprises a processor, at least one actuator coupled to the processor, a clock capable of generating the time element, a memory element configurable to store the private key and public key information (such as the key identifier), a signature generator coupled to the processor operable to generate a digital signature, and an emitter coupled to the signal generator operable to emit the secure identifier. In an aspect of an embodiment, multiple digital signatures using multiple cryptographic keys may be stored or generated by a storage element and utilizing the processor.

[0013] A process that the apparatus undergoes to transmit a secure identifier comprises generating a time element, selecting a key identifier, generating a random number, generating a digital signature as a function of a private key, the time element, and the random number; and emitting the data packet.

[0014] An apparatus that may be used to receive an authentication message comprises a receiver configurable to receive a secure identifier. The secure identifier comprises a public key identifier, a time identifier, and a digital signature. The apparatus further comprises a verifier configurable to verify the secure identifier. The verifier comprises memory comprising at least one public key and information relating to time tolerances and access privileges, a key retriever configurable to retrieve the public key and access privileges associated with the public key, a time verifier configurable to verify that the received time identifier falls within the time tolerances, and a digital signature verifier. The digital signature verifier determines the authenticity of the digital signature as a function of the digital signature, the public key, and the time identifier. The digital signature may further be encrypted with a PIN where the receiver decrypts the digital signature using PIN information accessed in association with the public key.

[0015] A process undergone to receive a secure identifier comprises receiving a secure identifier, the secure identifier comprising a digital signature, a public key identifier and a time identifier, and verifying the validity of the secure identifier.

[0016] In another aspect, the apparatus may further comprise a key selector to select the particular key within the device.

[0017] In another aspect, it is an advantage to provide an authentication device and method that only requires communication in one direction.

[0018] In another aspect, the apparatus and method may encrypt a digital signature using a personal identification number (PIN).

[0019] In another aspect, the transmitting device minimizes the information sent to the receiving device so that authentication may occur more quickly.

[0020] In another aspect, a sequence reference is included in the secure identifier to prevent replaying of the same secure identifier.

[0021] In another aspect, the apparatus and method may create public and private keys internally within the authentication device.

[0022] In another aspect, the apparatus and method provides for authentication without the use of the public key infrastructure.

BRIEF DESCRIPTION OF THE DRAWINGS

[0023] The features, objects, and advantages of the invention will become more apparent from the detailed description set forth below when taken in conjunction with the drawings in which like reference characters are identified correspondingly throughout and wherein:

[0024] FIG. 1A is a block diagram of a physical implementation of an audio authentication device;

[0025] FIG. 1B is a block diagram of another physical implementation of an audio authentication device;

[0026] FIG. 1C is a block diagram of a physical implementation of an optical authentication device;

[0027] FIG. 1D is a block diagram of a physical implementation of an authentication device;

[0028] FIG. 2 is a block diagram of a transmitting authentication device;

[0029] FIG. 3 is a flow chart of an authentication procedure;

[0030] FIG. 4 is a block diagram of a receiving authentication device;

[0031] FIG. 5 is a block diagram of a receiving authentication procedure; and

[0032] FIG 6 is a block diagram of an authentication device integrated into a wireless phone.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0033] An authentication device may be used to verify the identity of an individual to allow transactions between the individual and various external devices. In particular, the authentication process is one-way; that is, the individual transmits a secure identifier, the receiver then authenticates the secure identifier, and permits access. Physical possession and operation of the authentication device provides one aspect of the required verification, in much the same manner

that the physical possession of a key allows an individual to gain access through a locked door. Optionally, for more secure applications, the authentication device may be combined with an application-specific password or personal identification number (PIN).

[0034] The authentication device may be small enough to attach to a key ring. Alternatively, the authentication device may be embedded into another device, such as a wireless phone or a personal data assistant (PDA). In one mode of operation, the user may hold the authentication device near a receiver, or an input device. Actuating the device, such as pressing a button, activates the authentication device, thereby emitting a short signal that identifies the token in a cryptographically secure manner. The signal encodes a cryptographically secure message, or a secure identifier, and preferably uses public key technology, although the public key infrastructure may also be bypassed. The secure identifier may include a representation of the time. Receipt and verification of the secure identifier proves that the signal was sent by the token. Checking the time encoded within the secure identifier to be within reasonable limits of the time as known in the receiver provides evidence that the audio signal simply is not a replay of a recorded signal at a later time.

[0035] One method for generating digital signatures is public-key cryptography. In a public-key cryptography scheme, a user has both a private key for signing and a public key for verification. The user signs a communication with the user's private key and sends the secure identifier with the communication to a targeted party, which then verifies the communication with the user's public key. The fact that the targeted party is able to verify the communication with the user's public key is the electronic signature that authenticates the communication as originating from the user. It should be noted that use of a public-key cryptography scheme is illustrative only and the exemplary embodiments may incorporate other proof of knowledge schemes.

[0036] In another non-limiting exemplary embodiment, the public key infrastructure is bypassed. A one-time meeting to identify the individual who wishes to gain access occurs. In an example of security to allow a person to access buildings, an individual would go to a security office and satisfy the security office of his or her identity. Upon satisfaction of the individual's identity, the individual activates her personal security device, which causes the device to transmit the public key information corresponding to the private information contained within her personal security device. The public key information is received by the security office and recorded and stored.

[0037] In operation, when the individual attempts to gain entry, the individual activates the security device, thereby transmitting the secure identifier towards a receiving device, which in turn verifies that the transmitted signal received is verified using the public key which was recorded and stored in the security office. Access information and privileges information may be

stored in association with the public key. In an embodiment, the receiver is coupled to a security database that uses a short identifier such as a database index. A time stamp in the secure identifier transmitted further verifies that the transmission signature falls within acceptable time limits as received, thereby allowing entry. Moreover, the secure identifier may be verified such that the time indicated is later than the last time the signature was used. This prevents the replay of the same signature, even if just a short time later. In an embodiment, the time tolerances are predetermined. Upon verification, access is allowed. Accordingly, a transmitted secure identifier is authenticated using one-way communication.

[0038] It should be noted that in situations where greater anonymity is desirable, the individual may provide another secure identifier to a receiving device, one which does not have her name corresponding to the secure identifier transmitted. For example, a second secure identifier may be generated, using a key that was initially set-up not to include the name of the individual.

[0039] In another mode of operation, which may be more applicable for higher security applications, the user may also be required to enter a personal identification number (PIN) code. As such, use of the PIN acts as a first unlocking of a device. In addition, a PIN code may also be entered directly into the receiving or verifying device, such as that found in an ATM machine. Further, it is contemplated that a user may have different PINs for different applications, such that even if the PIN code was discovered for one application, the same PIN code may not allow access to other devices. The PIN code may be entered either before or after the audio signal is transmitted, and may be entered either to the device generating the signal, or to the device receiving the signal.

[0040] In another higher security mode of operation, the verifier, or receiver, conveys to the user a challenge to be signed together with the time element. The challenge is preferably random, and therefore likely to be unique for each occurrence. For example, the receiver may have a display asking the user to input a series of numbers (challenge) into the authenticating device. The user then enters the challenge into the authenticating device and activates it to sign the challenge, together with the time element. Thus, the digital signature of the challenge, together with the time element, provides greater protection against replay attacks. For example, replaying a recorded message to a verifier, even within acceptable time tolerances, will not succeed as long as the verifier chooses a different challenge.

[0041] In an embodiment, the authentication device comprises a single actuator. In alternate embodiments, multiple actuators may be present on the device to select different internal cryptographic keys or provide other user interfaces. When activated, an authentication signal is emitted. Information that may be encoded in the signal includes a key identifier. A key

identifier may have a device serial number and a predetermined quantity of the bits selecting the particular key within the device, or the key identifier may be a hash of the public key. Other information that may be encoded includes a predetermined quantity of bits representing the time as represented in the device. In another embodiment, the least significant bits of the time in the device are utilized.

[0042] The receiving device demodulates and verifies the signal (including verifying the signature and verifying the time). The authentication receiver has pre-stored a record of the public key corresponding to the secret key in the device, among other information, in particular, information about the amount of acceptable clock drift, the last known drift, might be stored and taken into account. The record may also include attributes associated with the public key, such as the access privileges associated with that particular public key. Access privileges may be information such as, but not limited to, when and where a particular public key may be used. Access privileges may also include which devices the public key may have access to. Using information regarding clock drift and the least significant bits of the current time, the authentication server would determine the time that the digital signature applies to, and thus may verify the signature to allow access.

[0043] Alternatively, the receiving device may demodulate the signal and transmit the signal to a verifier located elsewhere. For example, a centralized verifier may receive the signals, in digital or analog form, and conduct the verification process. The centralized verifier may comprise a central, backend database containing information needed to verify received signatures and associated privilege information. Upon verification, the centralized verifier sends the necessary information to the authentication receiver. Thus, the demodulation of the received secure identifier and the verification of the signature may occur in two places – either in the receiving device or in the centralized verifier/database.

[0044] In another embodiment, the authentication device is provisioned with more than one key and may have the ability to create additional keys internally. In such embodiments, an internal random number generator is used to create keys within the authentication device.

[0045] Figure 1A illustrates a block diagram of a physical implementation of an authentication device 100. The device 100 comprises an activator or actuator 104. Optionally, additional actuators 108 and 112 may also be used. Additional actuators 108 and 112 may be used to activate different keys, which in turn, authenticate different applications. The actuators 104, 108 and 112 may be any type of switch, such as a push-button switch, a toggle switch, a dial, or a voice activated switch. An emitter 116 emits an audio authentication signal or secure identifier 120. The secure identifier 120 comprises a digital signature, an identifier of the public key to

gain access to a particular device, along with other information, such as the current time. In an embodiment, a predetermined number of bits represent the time. In another embodiment, a predetermined number of least significant bits represent the time. In so doing, receipt and verification of the secure identifier 120 is evidence that secure identifier 120 was sent by the authentication device 100. Further, a check of the time encoded in the secure identifier against the current time verifies that the time encoded is within reasonable limits of the current time. The digital signature is a function of the private key, and preferably of the key identifier, along with a random number. The private key corresponds to the specified public key. If the secure identifier 120 is being transmitted in response to a challenge, the digital signature is a function of the challenge.

[0046] Figure 1C illustrates a block diagram of an alternate physical implementation of an authentication device 124. An actuator 128, and optionally additional actuators 132 and 136, allow a user to select a particular key. An emitter 140 emits an optical authentication signal or secure identifier144.

[0047] In yet another embodiment, Figure 1B illustrates a physical implementation of another authentication device 148. A display 152 displays to the user the different keys that are selectable. Selector keys 156 and 160 allow the user to scroll and identify the various keys available. An actuator 164 allows the user to select the desired key to be emitted through an emitter 168. The emitted secure identifier 172 is in the form of an audio secure identifier or an optical secure identifier, is then emitted to a receiving device for authentication.

[0048] Figure 1D illustrates another embodiment of a physical implementation of an authentication device 176. Similar to the embodiment as illustrated in Figure 1B, display 180, along with selectors 184 and 188, allow a user to scroll through and identify various keys. A user input device, such as keypad 192, allows a user to input a personal identification number (PIN) in addition to the digital signature. An actuator 194 selects and sends the selected key in the form of an encrypted secure identifier through the emitter 196.

[0049] As used herein, a digital signature is a randomized function of the signer's private key and the message being signed. That is, a digital signature is a function of the signer's private key, the message being signed, and a random number. In one embodiment, a message is signed using the signer's private key. In this embodiment, the message being signed is usually the time identifier, although other information may be used. In an alternate embodiment of a challenge-response scenario, the message being signed is the challenge that the user has typed in (possibly together with the time identifier). Thus, in order to verify a digital signature, one needs the signer's public key, the signature to be verified, and the message that was signed. Thus, the "secure identifier"

that the token sends to the verifier contains the information necessary for verification: public key identifier (the key itself should be known to the verifier already), the message (i.e. the time identifier), and the signature.

[0050] In a non-limiting exemplary embodiment, audio tones are used to uniquely represent the cryptographic signatures stored on or generated by the authentication device. Many devices, such as desktop and laptop computers currently integrate or may be accessorized with the capability to generate or receive audio tones. Other electronic devices, such as personal data assistants (PDAs), mobile phones, pagers, and alarm systems may also be used with the exemplary embodiments with the proper accessories. In addition, other communication methods such as telephone networks, radio networks, intercom systems, Bluetooth™, other wireless means and other RF communication systems may be utilized. Accordingly, a user may use exemplary embodiments to identify him/herself directly in face-to-face transactions or indirectly through communication media.

[0051] In another non-limiting embodiment, optical signals are used to uniquely represent cryptographic signatures stored on or generated by the authentication device. Similar with respect to audio tones, many devices may be equipped or accessorized with the capability to generate or receive wireless signals, such as infrared, radio frequency, and optical signals.

[0052] Figure 2 illustrates a block diagram of the internal operations of an authentication device 200. An actuator 204 is coupled to a central processing unit (CPU) or processor and associated memory 208. The actuator 204 may be any type of user-enabled actuator, such as a toggle switch, a pushbutton switch, or voice-activated switch. The processor and memory 208 is coupled to an internal clock 212, a random number generator 216, and, optionally, additional static memory 220. Alternatively, random number generator 216 may be a pseudo-random number generator, based on a pre-loaded random seed. The clock 212 generates the time. Although the clock need not identify the current time, the time does have to be consistent with the receiver of the authentication signal. Also, the clock may have a separate supplemental or back-up power supply, such as a battery (not shown). That is, the time represented in the transmitting device and the receiving device need to advance at the same rate, but they may be offset from one another. Static memory 220 may be used for the storage of key identifiers and other information. Static memory is also useful when the power source (such as a battery) needs to be replaced. Of course, memory 208 may also be used for such storage.

[0053] Different key identifiers may be used to identify the user to allow for different transactions. For example, one key may be used for a bank to allow for transactions, another key may be specific to gain entry into car doors, another key for office doors, and so on. Similarly,

the same key identifier may be used for different transactions. Accordingly, the same key may be used to gain entry into specific office doors, car doors, a phone or a computer. The key identifiers that may be stored in memory 220 may include information, such as the device serial number and, potentially, a number of bits indicative of the particular key within the device.

[0054] Optionally, the device 200 may comprise an input device 228 capable of receiving a personal identification number (PIN). The PIN may be used in transactions where there is a perceived need for a greater level of security. The processor 208 generates a data packet, combining a predetermined number of bits representing the time, along with the appropriate key identifier, and generates an encrypted digital signature. The secure identifier is then output through an emitter, such as emitter 224. If the secure identifier is an audio secure identifier, the authentication device may be positioned proximate to an audio input device such that the receiver receives the audio secure identifier. Similarly, if the secure identifier is an optical secure identifier, the authentication device may be positioned proximate to an optical input device such that the receiver receives the optical secure identifier. It should be noted that the authentication device need not be proximate to the receiver. For example, in an example of using a telephone, the secure identifier is transmitted through emitter 224 into a phone transmission system (wired or wireless), to be received by a remote receiver.

[0055] In another embodiment, the PIN is entered directly into the receiving device, such as the case of an automated teller machine (ATM). In such a case, the PIN may be used to encrypt the signature part of the transmitted data (as opposed to the time stamp or the identifier). In another embodiment, the PIN is again input directly into the receiving device.

[0056] Figure 3 illustrates a flowchart of the operation of an authentication device described with respect to Figure 2. The time is generated 304. The particular key needed for a given operation is identified 308. A random number 312 is generated. A processor, such as the processor 208 of Figure 2, generates a digital signature 316 using the current time (time identifier), the identified private key, and the generated random number. Optionally, the digital signature generated is encrypted using the user-inputted PIN. The digital signature 316, coupled with the time identifier and a public key identifier, collectively called the secure identifier, is then emitted 324. It should be noted that the above steps may occur in any order.

[0057] Figure 4 illustrates a device that receives the secure identifier 400. A receiver 404 receives the emitted signal from the authentication device and demodulates the signal. The data is then forwarded to a verifier 408. The verifier 408 comprises memory 412, a time verifier 416, and a signature verifier 420. The memory 412 contains a record of the public key corresponding to the secret key in the device, and other information. In particular, information regarding the

amount of acceptable clock drift, the last known drift, and other time-related information may be stored and taken into account. Also, access and privileges information is stored in association with the public key. Thus, the time verifier 416 compares the time as received from the secure identifier with a predetermined time window of acceptance, also taking into account such clock drift information. If the time as received falls within acceptable time constraints, the time component of the secure identifier is verified. The public key corresponding to the public key identifier is also retrieved.

[0058] The signature verifier 420 preferable contains a processor and verifies that the signature generated by the private key corresponds to the stored public key. Optionally, a PIN verifier 424 verifies that the appropriate PIN was used, by decrypting the digital signature received as a function of the PIN. If the verification process is successfully completed, access to the device is allowed. No signal from the receiving device 400 needs to be sent to the emitting device in order for access to be allowed.

[0059] Figure 5 illustrates a flowchart of the process undergone by a device as described with respect to Figure 4. A secure identifier is received and demodulated 504. Optionally, the secure identifier is decrypted using the PIN 508. Step 512 verifies the digital signature. The public key corresponding to the public key identifier transmitted is accessed to determine the validity of the secure identifier using the accessed key. Step 516 verifies the time. The time indicated in the received secure identifier is verified to be within acceptable time tolerances as predetermined in the receiving device (or centralized verifier). If the signature, the time information and, optionally, the PIN information 520 is acceptable, access is allowed 524. Otherwise, the access requested is rejected 528. Note that, in the absence of the correct public key with which to verify the signature, a signature itself appears to be random data, and so an adversary who intercepted this could not verify guesses about the correct PIN, even though the link itself is not secure.

[0060] In another embodiment, the device may operate through a secure co-processor, such as a smart card or a Subscriber Identity Module (SIM card). In the non-limiting example of a SIM card and a wireless phone, the SIM card is inserted into a wireless phone 600, as illustrated in Fig. 6. The SIM card is the secure portion 604 and the remainder of the phone is the non-secure portion 608. Similar to the embodiment described in Fig.2, the SIM card houses an internal random number generator 612, memory for keys 616, a processor (and memory) 620 and, optionally, PIN module 622. The device takes advantage of inherent components in the wireless phone, such as an activator 624, a clock 628 and a signal output or transmitter 632. Alternatively, the clock 628 may reside within secure portion 604. In the situation where the clock 628 resides outside the secure portion 604, for example, a wireless code division multiple

access (CDMA) handset may derive its time component from the network. Thus, compromising of network time, or emulating network time to compromise the security of the handset (i.e., fool the handset), is more difficult.

[0061] It should be noted that the exemplary embodiments may be implemented whenever a database for storing information pertaining to the authentication process exists at the receiving end, or is accessible by the receiving end. The processor of the exemplary embodiments may be used to implement one cryptographic scheme with one party and another cryptographic scheme with another party. The basic implementation of the exemplary embodiments may be performed without the need for physical connection to intermediary resources because communication with separate parties occur through a wireless medium.

[0062] Those of skill in the art would understand that the various illustrative logical blocks, modules, circuits, and algorithm steps described in connection with the embodiments disclosed herein may be implemented as electronic hardware, computer software, or combinations of both. The various illustrative components, blocks, modules, circuits, and steps have been described generally in terms of their functionality,. Whether the functionality is implemented as hardware or software depends upon the particular application and design constraints imposed on the overall system. Skilled artisans recognize the interchangeability of hardware and software under these circumstances, and how best to implement the described functionality for each particular application. As examples, the various illustrative logical blocks, flowcharts, windows, and steps described in connection with the embodiments disclosed herein may be implemented or performed in hardware or software with an application-specific integrated circuit (ASIC), a programmable logic device, discrete gate or transistor logic, discrete hardware components, such as, e.g., registers in the FIFO, a processor executing a set of firmware instructions, any conventional programmable software and a processor, a field programmable gate array (FPGA) or other programmable logic device, or any combination thereof. The processor may advantageously be a micro-controller, but in the alternative, the processor may be any conventional processor, controller, micro-controller, or state machine. The software may reside in RAM memory, flash memory, ROM memory, EPROM memory, EEPROM memory, hard disk, removable disks, a CD-ROM, a DVD-ROM, registers, or any other magnetic or optical storage media. Those of skill of the art would further appreciate that the data, instructions, commands, information, signals, bits, symbols, and chips that may be referenced throughout the above description are advantageously represented by voltages, currents, electromagnetic waves, magnetic field or particles, optical fields or particles, or any combination thereof.

[0063] The previous description of the preferred embodiments is provided to enable any persons skilled in the art to make or use the present invention. Various modifications to these embodiments will be readily apparent to those skilled in the art, and the generic principles defined herein may be applied to other embodiments without the use of inventive faculty. Thus, the present invention is not intended to be limited to the embodiments shown herein, but is to be accorded the widest scope consistent with the principles and novel features disclosed herein.

[0064] What we claim as our invention is: